Computing isogenies between maximal abelian surfaces over $\mathbb{F}_{p^2}$ and applications in post-quantum cryptography

Julien Soumier

Internship report for M2 Algèbre Appliquée of Université de Versailles

September 25, 2023

Contents

Introduction

Environment

The CARAMBA project-team welcomed me at INRIA Nancy-Grand Est laboratory under the supervision of Pierre-Jean Spaenlehauer, research fellow at INRIA. Among the research themes studied by the team, we have chosen to start working on the use of abelian varieties in cryptography. The emergence of this theory in cryptography may come as a surprise, but in the next paragraph we try to explain why it is actually quite natural. I would particularly like to thank Pierre-Jean for his patience with all my questions, and for the time he took to read this document.

Context and Motivations

A cornerstone of modern cryptography is the Diffie-Hellman algorithm [DH], which allows two parties to *safely* agree on a shared key. It is based on the *discrete logarithm problem* (see [CFA, §1.5]). It was a very secure protocol until the advent of quantum algorithms and in particular Shor's [Sho]. This new type of quantum cryptanalysis is fast becoming a global concern, thanks largely to the development of quantum computers, and their media coverage. Some governments and companies want secure encryption, even against possible future technologies. This is where the main topic of this report comes in: *isogeny between abelian varieties*, where the abelian varieties first appears as elliptic curves.

Lucas De Feo, David Jao and Jérôme Plût proposed in [FJP] the SIDH (Supersingular Isogeny Diffie–Hellman) cryptosystem as a new and secure way to do key exchange. This protocol uses isogenies of elliptic curves, and relies on the fact that finding isogenies between supersingular elliptic curves is very hard even for quantum computers. This post-quantum alternative to the Diffie-Hellman algorithm was very promising, until the recent cryptanalysis breakthrough by [MMP$^+$], [CD] and [Rob]. The common idea of these three papers is to use Kani's notion of *isogeny diamond configuration* [Kan1]. These configurations are used in practice to construct isogenies of certain degrees (see Theorem 1.3.1) between abelian varieties of dimension greater than 1. Abelian varieties are *projective* varieties together with a group law given by *morphisms*. The first examples were elliptic curves, but now in the previous attacks on SIDH, we are working with products of such curves. For instance if E_1 and E_2 are elliptic curves over a finite field $\mathbb{F}_q$, then their product $E_1 \times E_2$ equipped with the component-wise group law, is an abelian variety of dimension 2. This is why we need to understand abelian variety theory, in order to work on these cryptographic protocols.

The authors of [FMP] have recently proposed a new key exchange system based on SIDH. It is called M-SIDH (Masked Supersingular Isogeny Diffie-Hellman), and is a candidate countermeasure to attacks based on Kani's theorems. The idea is to twist some parameters, in order to hide critical information. The final (and distant) goal of our work is to apply the algorithms we have developed to the cryptanalysis of M-SIDH.

Contributions

After carefully reading the M-SIDH countermeasure [FMP] to the previous attacks, we decided to focus on the analysis of this protocol. It seemed to us that understanding specific abelian varieties, namely the product $E_1 \times E_2$ of two maximal supersingular elliptic curves, is at the heart of the problem. More precisely, we want to compute isogenies between these abelian varieties. We work with the software MAGMA, a computer algebra system designed to solve mathematical problems. If the elliptic curve theory is already implemented in this software, we do not find any primitives to build higher-dimensional abelian varieties or isogenies. However, Lubicz and Robert described in [LR] an algorithm that computes isogenies between abelian varieties from a given kernel. This was then implemented by Bisson Cosset and Robert in the MAGMA package *AVIsogenies* [GB]. They work with objects such as theta structures, which seem too deep for this 6-month internship. So we decided to postpone our study of their work until later and concentrate first on the specific cases that interest us.

So we had to find a way to represent isogenies between products of elliptic curves in MAGMA, and to construct them from a given kernel. Since the abelian varieties we are working on are maximal, they always split as a product of elliptic curves (Theorem 1.2.7). Thus the higher-dimensional isogenies we compute come with a natural *matrix representation*, see Subsection 2.1.1. This way of implementing 2-dimensional isogenies raises many theoretical and practical questions (see Subsection 2.1.2). We reached a first step by implementing an algorithm which constructs a matrix of 4 morphisms (*i.e.* a morphism between 2 dimensional abelian varieties) from a finite kernel subgroup $K \subset E_1 \times E_2$. But the computations were too expensive, and our algorithm too slow.

Then we learned that there was an additional structure to take into account while working on abelian varieties, a *polarization*. We studied the properties that a finite subgroup of a product $E_1 \times E_2$ has with respect to a polarization (see Subsection 2.2.1). The matrix of morphisms $[f_{ij}]_{i,j}$ we obtained from such a kernel also has good properties. For instance, we found non-trivial relations between the degrees of the f_{ij}. Thanks to these observations we were able to speed up our algorithm. We now have encouraging results, but there are still many open questions that we need to investigate. For example, is there a bound on the degrees of the f_{ij}, depending on the cardinality of K? How do the *polarized structure* of abelian varieties behave with respect to isogenies between them? For precisions we refer to 2.2.4, the last section of this report.

Outline

This report is divided into two main chapters. First, we present some cryptographic work related to the SIDH protocol, as well as the basics of the theory of abelian varieties. In Section 1.1 we explain how SIDH works, and try to justify the choice of the parameters such as the elliptic curves, or the ground fields. Then in Section 1.2 we give facts to know about abelian varieties, although many of the theorems we will use will be black boxes. In the third and fourth sections (respectively 1.3 and 1.4) we describe the attacks of [MMP$^+$] and [Rob] against SIDH, then the M-SIDH countermeasure [FMP].

Secondly, in Section 2.1, we begin by explaining how we decided to represent the isogenies between product of elliptic curves. Then we describe an algorithm to construct such isogenies $\phi : E_1 \times E_2 \to E_1' \times E_2'$ from a finite subgroup $K \subset E_1 \times E_2$, where $\mathrm{Ker}(\phi) = K$. We have worked under certain conditions for the E_i, although these assumptions are always verified in our target

applications. Then in Section 2.2, we give some contributions about isogenies between products of two maximal elliptic curves defined over $\mathbb{F}_{p^2}$ for a prime p. Finally, we use these observations to speed up our first algorithm, by adding a structure on the abelian varieties $E_1 \times E_2$, and making a strong assumption on the kernel K of $\phi : E_1 \times E_2 \to E_1' \times E_2'$. This assumption is still verified in our application but leads to deeper theoretical questions, see Subsection 2.2.4.

1 Background

1.1 SIDH: a key exchange algorithm based on isogenies of supersingular elliptic curves

1.1.1 Context of the cryptosystem

We begin this report by describing the SIDH protocol, a potential new algorithm for post-quantum key exchange. In order to describe the work of [FJP], we need to know basic facts about elliptic curves. For an introduction to this theory, we recommend these two complementary books: [Was] and [Sil].

For our protocol we need to fix a first curve E_0 over a finite field $\mathbb{F}_q$, with some *nice properties*. First, it needs to be *supersingular*. Indeed such curves bring safe properties with them:

- The isogeny graph is a *Ramanujan graph* (See [Feo],[LPS]) meaning it is a highly connected sparse graph. It increases the complexity of computing isogeny paths.

- There is no natural abelian group action on the set of supersingular curves with fixed endomorphism ring $\mathcal{O}$. Contrary to the action of $Cl(\mathcal{O})$ in the ordinary case, which can be useful for quantum cryptanalysis. [Feo].

Moreover, we want that E_0 has many rational subgroups. More precisely, if we denote by ℓ_a, ℓ_b two distinct prime numbers and e_a, e_b two positive integers, we want that there exists subgroups of $E_0(\mathbb{F}_q)$ of order $\ell_a^{e_a}$ and $\ell_b^{e_b}$. These subgroups represent *walks* in the two graphs where vertices are isomorphism classes of elliptic curves, and edges are isogenies of degree ℓ_a and ℓ_b respectively. Indeed, thanks to Vélu's formula [Was, Theorem 12.16], we have the effective correspondence:

$$\begin{gathered}\text{Finite subgroup } K \subset E_0(\mathbb{F}_q) \text{ of order } \ \ell \\ \longleftrightarrow \\ \text{Isomorphism class of isogenies } \ \phi : E_0 \to E' \text{ where } \mathrm{Ker}(\phi) = K \text{ and } \deg(\phi) = \ell.\end{gathered}$$

If $E_0(\mathbb{F}_q)$ has many subgroups of order ℓ, then there are many non-isomorphic degree ℓ isogenies of domain E_0. So if someone's secret is a ℓ-isogeny of domain E_0, it may be computationally hard for an attacker to find it. The following theorem provides a way to control the group structure of $E_0(\mathbb{F}_q)$ so that it has many rational subgroups of order $\ell_a^{e_a}$ and $\ell_b^{e_b}$.

Theorem 1.1.1. *[Feo] We can choose $p = \ell_a^{e_a}\ell_b^{e_b} f \mp 1$ and E_0 supersingular such that*

$$E_0(\mathbb{F}_{p^2}) \simeq \left(\mathbb{Z}/(p \pm 1)\mathbb{Z}\right)^2 \simeq \left(\mathbb{Z}/(\ell_a^{e_a}\ell_b^{e_b} f)\mathbb{Z}\right)^2$$

Where $f \in \mathbb{Z}_{\geq 0}$, is a small cofactor.

In practice, to construct such p we try with different values of f and then test their primality using for instance the Miller-Rabin probabilistic algorithm. We may often choose $f = 1$, from now on we work under this assumption. Thanks to the previous theorem, the $\ell_a^{e_a}$ and $\ell_b^{e_b}$-torsion subgroups are rational, and we can compute one of their basis (as $\mathbb{Z}/\ell_a^{e_a}\mathbb{Z}$ and $\mathbb{Z}/\ell_b^{e_b}\mathbb{Z}$ free modules of rank 2) in $E_0(\mathbb{F}_{p^2})$. Otherwise we may have to work in an extension of $\mathbb{F}_q$, which would slow the computations. Let $(P_a, Q_a) \in E_0(\mathbb{F}_{p^2})^2$ (resp. (P_b, Q_b)) denote a basis of the module $E_0[\ell_a^{e_a}]$ (resp. $E_0[\ell_b^{e_b}]$).

1.1.2 SIDH protocol

Let us describe the cryptosystem itself, with E_0 as in Theorem 1.1.1. In our description, Alice and Bob want to compute a shared key. This secret will be an (isomorphism class of an) elliptic curve $E_{a,b}$, computed by both Alice and Bob, using their respective private keys.

Private Settings
Alice chooses a torsion point $A = [m_a]P_a + [n_a]Q_a$ and computes the isogeny $\phi_A : E_0 \to E_0/\langle A\rangle = E_a$.
Bob chooses a torsion point $B = [m_b]P_b + [n_b]Q_b$ and computes the isogeny $\phi_B : E_0 \to E_0/\langle B\rangle = E_b$.
Exchange
Alice sends $(E_a, \phi_A(P_b), \phi_A(Q_b))$ to Bob.
Bob sends $(E_b, \phi_B(P_a), \phi_B(Q_a))$ to Alice.
Computation of shared key
Alice computes $\phi_B(A) = \phi_B([m_a]P_a + [n_a]Q_a) = [m_a]\phi_B(P_a) + [n_a]\phi_B(Q_a)$.
And then $E_b/\phi_B(A) \cong E_0/\langle A, B\rangle = E_{a,b}$.
Bob computes $\phi_A(B) = \phi_A([m_b]P_b + [n_b]Q_b) = [m_b]\phi_A(P_b) + [n_b]\phi_A(Q_b)$. And then $E_a/\phi_A(B) \cong E_{a,b}$.

$$\begin{array}{ccc} E_0 & \xrightarrow{\phi_A} & E_a \\ {\scriptstyle \phi_B}\downarrow & & \downarrow{\scriptstyle \bmod \phi_A(B)} \\ E_b & \xrightarrow[\bmod \phi_B(A)]{} & E_{a,b} \end{array}$$

That way, Alice and Bob both know the isomorphism class of $E_{a,b}$, which can be encoded via its j-invariant. Alice because she knows the action of ϕ_B on the $\ell_a^{e_a}$-torsion group, and symmetrically for Bob. We hoped that this additional information about the torsion points would not be a threat to the protocol security, *i.e.* that knowing $(E_a, \phi_A(P_b), \phi_A(Q_b))$ it is still hard to compute ϕ_A and its kernel (see Problem 1.3). This hope collapsed recently with the articles [MMP$^+$] and [Rob].

1.2 Products of isogenous elliptic curves

To understand the attacks described in [Rob], [MMP$^+$] and [CD] we need to give some basis of abelian variety theory. The book [HS] is an accessible introduction to this theory, and we can find more advanced theorems in [Mil] and [Mum]. We also give specific results on abelian varieties which are isomorphic to a product of elliptic curves, because they appear in the cryptanalysis of SIDH.

1.2.1 Abelian varieties

First properties

Intuitively an abelian variety is a projective variety together with a group structure. The most familiar example is an elliptic curve, indeed it is a projective curve by definition and we can construct the usual group structure on its points. As we see, this notion is at the intersection of the group and variety theories. We give a definition mixing both worlds:

Definition 1.2.1. If k is a field, a *k-algebraic group* is a tuple (G, e, m, i) where:

- G is a variety defined over k
- e is a point in $G(k)$ (the neutral element)
- $m : G \times G \to G$ a morphism (the group law on G)
- $i : G \to G$ a morphism (giving the inverses)

satisfying the *group axioms*: for all $x, y, z \in G$,

$$\begin{aligned} &m(e, x) = m(x, e) = x \\ &m(i(x), x) = m(x, i(x)) = e \\ &m(m(x, y), z) = m(x, m(y, z)) \end{aligned}$$

Since an algebraic group has a group structure defined by morphisms, as in Lie group theory, proving certain properties on *one* point is sufficient to show it on the whole group *by translation.*

Proposition 1.2.1. *[HS, §A.1.4] If (G, e, m, i) is a k-algebraic group, then it is a* smooth *variety.*

Abelian varieties are special cases of algebraic groups.

Definition 1.2.2. An *abelian variety* over a field k is a k-algebraic group where the underlying variety is projective.

The fact that the variety is projective rigidifies the structure, making abelian varieties satisfy very strong properties. For example, there are algebraic groups which are not abelian such as $GL_n(\mathbb{R})$, but projective algebraic groups must be abelian. This explains the name "abelian variety".

Proposition 1.2.2. *[HS, Lemma A.7.1.3]. The law group on an abelian variety is* abelian

Now we will denote the law group on abelian varieties as usual by $+, -$, instead of m, i. Here and subsequently, $\mathcal{A}$ and $\mathcal{B}$ denote abelian varieties over a field k. After defining mathematical objects, we define arrows between them.

Definition 1.2.3. We call a k-morphism between the underlying varieties of $\mathcal{A}$ and $\mathcal{B}$ a *k-morphism of abelian varieties*, if it is also a morphism for their group structures. The set of k-morphisms of abelian varieties from $\mathcal{A}$ to $\mathcal{B}$ is denoted by $\mathrm{Hom}_k(\mathcal{A}, \mathcal{B})$.

Remark 1.2.1. As for the elliptic curves, every morphism from $\mathcal{A}$ to $\mathcal{B}$ is a morphism of abelian varieties up to translation [CFA, §4.3.3]. Once again the proof is based on the fact that the varieties are projective.

Let us focus on the main sub-family of abelian variety morphisms: isogenies. These morphisms are *almost* isomorphisms, and the obstruction can be estimated by the cardinality of their kernel.

Definition 1.2.4. A morphism of abelian variety $\phi \in \mathrm{Hom}_k(\mathcal{A}, \mathcal{B})$ is a *k-isogeny* when $\mathrm{Ker}(\phi)$ is finite and ϕ is surjective.

When we do not specify the field for an isogeny, it implicitly means that it is the definition field of the abelian variety considered (k in our case). The most common example is the multiplication by an integer, since the law group is abelian. Let us denote the multiplication by $n \in \mathbb{Z}$:

$$\begin{array}{rccc} [n]: & \mathcal{A} & \to & \mathcal{A} \\ & P & \mapsto & n \cdot P \end{array}$$

Since an isogeny is a homomorphism, we can define its kernel as usual. In the case of $[n]$, let us denote:

$$\mathcal{A}[n] := \mathrm{Ker}([n]).$$

Definition 1.2.5. Let $\phi : \mathcal{A} \to \mathcal{B}$ be an isogeny. We denote by $\deg(\phi)$ the *degree* of ϕ, being its degree as a morphism.

As abelian varieties are generalizations of elliptic curves, the methods used for the following proofs are similar.

Theorem 1.2.1. *[HS, Theorem A.7.2.7] Let d denote the dimension of $\mathcal{A}$ (as a variety), and p the characteristic of k.*

i) The degree of $[n]$ is n^{2d}.

ii) If $p = 0$ or $p \nmid n$ then

$$\mathcal{A}[n] = \mathrm{Ker}([n]) \simeq (\mathbb{Z}/n\mathbb{Z})^{2d}.$$

iii) If $p > 0$ then there exists $r \in [\![0, d]\!]$ such that for all $t \in \mathbb{Z}_{\geq 0}$:

$$\mathcal{A}[p^t] = \mathrm{Ker}([p^t]) \simeq (\mathbb{Z}/p^t\mathbb{Z})^r.$$

We must distinguish the case $p|n$ from the others. This is explained by the fact that $[n]$ is a *separable isogeny* if and only if $p \nmid n$.

Definition 1.2.6. Let $\phi : \mathcal{A} \to \mathcal{B}$ be an isogeny. We say that ϕ is *separable* when it is as a morphism of varieties.

In this work we consider only separable isogenies on finite fields. They have a lot of properties that make them less complicated to manipulate. For example, one of the main properties of separable isogenies, is that:

$$\deg(\phi) = \#\mathrm{Ker}(\phi).$$

We also recall that for isogenies $\phi_1 : \mathcal{A}_1 \to \mathcal{A}_2$ and $\phi_2 : \mathcal{A}_2 \to \mathcal{A}_3$, $\deg(\phi_2 \circ \phi_1) = \deg(\phi_2)\deg(\phi_1)$.

Duality and polarizations

Unless otherwise stated, we will abbreviate separable isogeny to isogeny. Let us generalize the notion of *dual isogeny* to abelian varieties. The major obstruction compared to elliptic curves is that the degree 0 part of its Picard group $Pic^0(\mathcal{A})$ is not longer isomorphic to $\mathcal{A}$ in general. We also must construct Pic^0 with other objects than divisors, but we do not show the details here. See [Mil] for more information. We do not recall the construction of the *dual* of an abelian variety, but let us summarize the facts we need:

Theorem 1.2.2. *[Mil, Section I.8] For any abelian variety $\mathcal{A}$, there exists a unique abelian variety denoted $\hat{\mathcal{A}}$ called its* dual*, such that the mapping $\mathcal{A} \mapsto \hat{\mathcal{A}}$ is* functorial*, and we have:*

$$\hat{\hat{\mathcal{A}}} \simeq A.$$

Moreover we can understand the group law on $\hat{\mathcal{A}}$ thanks to the group *isomorphism: $\hat{\mathcal{A}}(k) \simeq Pic^0(\mathcal{A})$.*

Now, for each abelian variety $\mathcal{A}$ we can functorially attach to it a dual abelian variety $\hat{\mathcal{A}}$. But how do this varieties interact with each other? To answer this question we must introduce the notion of *polarization*. Once again, we will not give the explicit definition, but the idea is the following:

A polarization on an abelian variety $\mathcal{A}$ is an isogeny $\lambda : \mathcal{A} \to \hat{\mathcal{A}}$ which comes from a *geometrical construction*.

The exact construction may be found in [Mil] §I.11, but it is not necessary to understand it for our purpose. Indeed we will only use a very specific polarization, which is explicit. Moreover, we use this notion with the aim of computing 2-dimensional isogenies that satisfy some properties (for instance, having a maximal isotropic kernel, see Definition 1.2.3), but we do not need to construct polarizations. This notion is an additional structure which helps to speed up computations. Even if the modern abstract definition of a polarization may be hard to grasp, in the case of *complex* abelian variety they naturally arise from the early work of Riemann on complex tori.

Definition 1.2.7. If a polarization $\lambda : \mathcal{A} \to \hat{\mathcal{A}}$ is an isomorphism, we say that λ is a *principal polarization*. And we call *principally polarized abelian variety* a couple $(\mathcal{A}, \lambda)$ where $\mathcal{A}$ is an abelian variety and $\lambda : \mathcal{A} \to \widehat{\mathcal{A}}$ is a principal polarization.

Remark 1.2.2. In dimension 1, $\mathcal{A}$ is E an elliptic curve, so we always have $E \simeq Pic^0(E) \simeq \hat{E}$, and hence E is *canonically* principally polarized. By slight abuse of notation we will identify $\hat{E}$ with E, and the canonical polarization with Id_E. In this case, we have the usual duality theorem:

Theorem 1.2.3. *[Sil, III, Theorem 6.1] Let E, F be elliptic curves over the same field k, and $\phi : E \to F$ an isogeny of degree d. There exists a unique isogeny $\hat{\phi} : F \to E$ called its* dual *such that:*

$$\phi \circ \hat{\phi} = [m].$$

In higher dimensions the situation is a bit more complicated. However, since the association $\mathcal{A} \mapsto \hat{\mathcal{A}}$ is functorial, every isogeny $\phi : \mathcal{A} \to \mathcal{B}$ is associated with a unique isogeny $\hat{\phi} : \hat{\mathcal{B}} \to \hat{\mathcal{A}}$. It is called the *dual* isogeny of ϕ, and we have [Mum, Corollary 4, §13]:

$$\deg(\phi) = \deg(\hat{\phi}). \tag{1.1}$$

Weil Pairing

Let E be an elliptic curve over a finite field k of characteristic p. From usual elliptic curves theory, for every $n \in \mathbb{Z}_{\geq 0}$ prime to p, one can define the *n-Weil pairing* over E as a nondegenerate, skew-symmetric bilinear form:

$$e_n : E[n] \times E[n] \to \mu_n(\overline{k})$$

where $\mu_n(\overline{k})$ is the group of n-roots of unity in an algebraic closure $\overline{k}$ of k.

We also have a Weil pairing on general abelian varieties, we do not explicit the construction here, but we recall the basic properties. It is important to notice that its domain is not in $\mathcal{A} \times \mathcal{A}$, but in $\mathcal{A} \times \hat{\mathcal{A}}$. For more details, see [Mil, I.13].

Theorem 1.2.4. *Let $\mathcal{A}$ be an abelian variety over a finite field k of characteristic p. Let $n \in \mathbb{Z}_{\geq 0}$ be an integer prime to p. There is a non-degenerated skew-symmetric bilinear form:*

$$e_{n,\mathcal{A}} : \mathcal{A}[n] \times \hat{\mathcal{A}}[n] \to \mu_n(\overline{k})$$

Such that if $\phi : \mathcal{A} \to \mathcal{B}$ is an isogeny, then the following relation between the pairing on $\mathcal{A}$ and $\mathcal{B}$ holds:

$$e_{n,\mathcal{A}}(P, \hat{\phi}(Q)) = e_{n,\mathcal{B}}(\phi(P), Q)$$

Since $\hat{\mathcal{A}}$ is at the heart of this definition, we naturally want to combine it with a polarization, in order to have a more familiar pairing.

Definition 1.2.8. Let $(\mathcal{A}, \lambda)$ be a polarized abelian variety. We define the (n, λ)-Weil pairing as:

$$\begin{array}{rccl} e^{\lambda}_{n,\mathcal{A}} : \mathcal{A} \times \mathcal{A} & \to & \mu_n(\overline{k}) \\ (P, Q) & \mapsto & e_{n,\mathcal{A}}(P, \lambda(Q)) \end{array}$$

To simplify notation we will frequently write e_n for $e^{\lambda}_{n,\mathcal{A}}$, and call this bilinear form the Weil pairing instead of the (n, λ)-Weil pairing, if it does not lead to any ambiguity. It might seem that we complicate the definition of the pairing by mixing it with a polarization. But in our case we will use only a specific polarization that make the pairing easy to compute.

Let us introduce a new concept that plays a key role in Section 2.2.1.

Definition 1.2.9. Let $e^{\lambda}_{n,\mathcal{A}} = e^{\lambda}_n$ be the (n, λ)-Weil pairing on a polarized abelian variety $(\mathcal{A}, \lambda)$ of dimension d. We call a finite subgroup $K \subset \mathcal{A}[n]$ *isotropic* for e^{λ}_n when:

$$\forall\, P, Q \in \mathcal{A}[n]\ e^{\lambda}_n(P, Q) = 1.$$

If in addition $\#K = n^d$, we say that K is *maximal isotropic*.

Remark 1.2.3. Another definition could have been given. We could say that a group is maximal isotropic when it is maximal for the inclusion among isotropic groups. One can check that these definitions are equivalent, see [Kan1, Proof of Proposition 1.1] and [Mum, Section 23].

Isogenies which respect a polarization

By considering *polarized* abelian varieties, we define another type of *dual isogeny*, which behave in a more familiar way.

Definition 1.2.10. Let $(\mathcal{A}_i, \lambda_i)_{i\in\{1,2\}}$ be two principally polarized abelian varieties, linked by a separable isogeny $\phi : \mathcal{A}_1 \to \mathcal{A}_2$. The *adjoint isogeny* $\tilde{\phi}$ of ϕ, *with respect to the polarizations* λ_1 and λ_2, is:

$$\tilde{\phi} = \lambda_1^{-1} \circ \hat{\phi} \circ \lambda_2$$

Since we will study products of abelian varieties, we want to know how the map $f \mapsto \tilde{f}$ interacts with the Cartesian product. This will be explained in Proposition 2.1.1.

Definition 1.2.11. With the same notation as above, we say that ϕ is an *N-isogeny* with respect to λ_1 and λ_2 when:

$$\tilde{\phi} \circ \phi = [N]$$

We will often abbreviate *N-isogeny with respect to* λ_a *and* λ_b to *N-isogeny*. This definition is motivated by concrete properties of the 2-dimensional isogenies considered in our analysis of M-SIDH.

Remark 1.2.4. For an N-isogeny $\phi : \mathcal{A} \to \mathcal{A}'$, we have

$$\mathrm{Ker}(\phi) = \tilde{\phi}(\mathcal{A}'[N])$$

Especially for elliptic curves, every separable isogeny of degree d is a d-isogeny, thus we can recover an (isomorphism class of) isogeny by the action of its adjoint on some torsion points.

Proof. Let $P \in \mathrm{Ker}(\phi)$. $\tilde{\phi}$ being surjective, $P = \tilde{\phi}(Q)$ for some $Q \in \mathcal{A}'$.

Furthermore $0 = \phi(P) = \phi \circ \tilde{\phi}(Q) = N \cdot Q$, and then $Q \in \mathcal{A}'[N]$. On the other hand if $P \in \tilde{\phi}(\mathcal{A}'[N])$, then $P = \tilde{\phi}(Q)$ for $Q \in \mathcal{A}'[N]$.

Thus $\phi(P) = \phi \circ \tilde{\phi}(Q) = N.Q = 0$, and finally $P \in \ker \phi$. □

The following proposition gives a computable necessary condition on the kernel of a N-isogeny.

Proposition 1.2.3. *[Rob, §3.1] Let $(\mathcal{A}_i, \lambda_i)_{i\in\{1,2\}}$ be two principally polarized abelian varieties, and $\phi : \mathcal{A}_1 \to \mathcal{A}_2$ a N-isogeny with respect to λ_1 and λ_2, and let K be its kernel. Then K is maximal isotropic for the (N, λ_1)-Weil pairing.*

Proof. Let $x, y \in K$. By Remark 1.2.4, we know that there exist $x', y' \in \mathcal{A}_2[N]$ such that $y = \phi(\tilde{y'})$ and $x = \phi(\tilde{x'})$. Theorem 1.2.4 justifies the next computations:

$$\begin{aligned} e_N^{\lambda_1}(x,y) &= e_N^{\lambda_1}(\phi(\tilde{x'}), \phi(\tilde{y'})) \\ &= e_N^{\lambda_2}(x', \phi \circ \phi(\tilde{y'})) \\ &= e_N^{\lambda_2}(x', Ny') \\ &= 1 \quad \text{because } y' \in \mathcal{A}_2[N] \end{aligned}$$

This proves that K is isotropic. Now ϕ is a N-isogeny ($\phi \circ \tilde{\phi} = [N]$), thus we have the equality of degrees $\deg(\phi)\deg(\hat{\phi})\deg(\lambda_1)\deg(\lambda_2) = N^{2\dim \mathcal{A}}$ by Theorem 1.2.1. But the λ_i are isomorphisms (and assumedly separable), so $\deg(\lambda_i) = 1$. Finally by Equation (1.1) we have $\deg(\phi)^2 = N^{2\dim \mathcal{A}}$ and then $\#K = \deg(\phi) = N^{\dim \mathcal{A}}$. Thus K is maximal isotropic. □

1.2.2 Products of elliptic curves

Let $(\mathcal{A}_i, \lambda_i)_{i\in\{1,2\}}$ be two principally polarized abelian varieties over a field k. We describe an operation to construct a new polarization on their product. First let us denote by $\mathcal{A} := \mathcal{A}_1 \times \mathcal{A}_2$ the product abelian variety, and $p_i : \mathcal{A} \to \mathcal{A}_i$ the projections for $i \in \{1, 2\}$. We refer to [Kan3, §11] for proofs.

Lemma 1.2.1. *The isogeny*

$$\begin{array}{rcl} p : \hat{\mathcal{A}}_1 \times \hat{\mathcal{A}}_2 & \to & \hat{\mathcal{A}} \\ (x, y) & \mapsto & \hat{p_1}(x, 0) + \hat{p_2}(0, y) \end{array}$$

is an isomorphism.

With this we state:

Theorem 1.2.5. *We define a principal polarization $\lambda_1 \otimes \lambda_2$ on $\mathcal{A}$ as the composition:*

$$\mathcal{A} \xrightarrow{(\lambda_1,\lambda_2)} \hat{\mathcal{A}}_1 \times \hat{\mathcal{A}}_2 \xrightarrow{p} \hat{\mathcal{A}}$$

$\lambda_1 \otimes \lambda_2$ is called the product polarization *of λ_1 and λ_2.*

Hence when we have $(E_1, \lambda_1), \ldots, (E_n, \lambda_n)$ principally polarized elliptic curves over a field k, we can endow the product $E_1 \times \cdots \times E_n$ with a canonical principal polarization: $\lambda_1 \otimes \cdots \otimes \lambda_n$. Moreover let us denote by $\mathcal{A}$ the product $E_1 \times E_2$, then for n prime to the characteristic of k, we can compute the Weil pairing on $\mathcal{A}$ with the pairings on E_1 and E_2.

Proposition 1.2.4. *With the same notation as above, for all $P = (P_1, P_2)$ and $Q = (Q_1, Q_2)$ in $\mathcal{A}$ we have:*

$$e_{n,\mathcal{A}}^{\lambda_1\otimes\lambda_2}(P, Q) = e_{n,E_1}(P_1, Q_1) \cdot e_{n,E_2}(P_2, Q_2)$$

For a proof, see [Mum, Section 23, page 228].

Remark 1.2.5. This equation leads to practical computations on the product $E = E_1 \times E_2$. For example, if we want to test whether a subgroup K of E is isotropic for $e_n^{\lambda_1 \otimes \lambda_2}$, it is enough to check that:

$$\forall P = (P_1, P_2),\, Q = (Q_1, Q_2) \in K \quad e_{n,E_1}(P_1, Q_1) \cdot e_{n,E_2}(P_2, Q_2) = 1$$

1.2.3 Maximal abelian varieties over $\mathbb{F}_{p^2}$

In this section we fix a prime p, and denote $q = p^m$ for some integer m. First we recall a theorem from Weil, which is the analog of the Riemann hypothesis on abelian varieties. The proof is hard, and can be found in [Mil].

Theorem 1.2.6. *[Mil, II,Theorem 1.1] Let $\mathcal{A}$ be an abelian variety of dimension g over a finite field $\mathbb{F}_q$. There are integers $a_1, \ldots, a_{2g}$ such that:*

i) For all $i \in [\![1, 2g]\!]$, $|a_i| = \sqrt{q}$.

ii) $\#\mathcal{A}(\mathbb{F}_q^m) = \prod_{i=1}^{2g}(1 - a_i^m)$.

For our purposes, as in SIDH (and later on M-SIDH), we will only consider abelian varieties over $\mathbb{F}_{p^2}$. The above theorem provides a bound on the number of rational points on such a variety.

Corollary 1.2.1. *Let $\mathcal{A}$ denote a g-dimensional abelian variety over $\mathbb{F}_{p^2}$. Then:*

$$(p-1)^{2g} \leq \#\mathcal{A}(\mathbb{F}_{p^2}) \leq (p+1)^{2g}$$

Proof. From Theorem 1.2.6 with $q = p^2$ and $m = 2$ we have:

$$\#\mathcal{A}(\mathbb{F}_{p^2}) \leq |\prod_{i=1}^{2g}(1 - a_i)| \leq \prod_{i=1}^{2g}(1 + |a_i|) \leq (1+p)^{2g}$$

and

$$\#\mathcal{A}(\mathbb{F}_{p^2}) \geq |\prod_{i=1}^{2g}(1 - a_i)| \geq \prod_{i=1}^{2g}(|a_i - 1|) \geq \prod_{i=1}^{2g}(|a_i| - |1|) \geq (p-1)^{2g}$$

□

Remark 1.2.6. There exist abelian varieties that meet those limits. For example, we can construct the product of elliptic curves that reach the Hasse-Weil bound. The main theorem of this section states that these are the only examples, up to isomorphism.

Definition 1.2.12. We call an abelian variety $\mathcal{A}$ over $\mathbb{F}_{p^2}$ *maximal* if $\#\mathcal{A}(\mathbb{F}_{p^2}) = (p+1)^{2\dim(\mathcal{A})}$. We call it *minimal* if $\#\mathcal{A}(\mathbb{F}_{p^2}) = (p-1)^{2\dim(\mathcal{A})}$.

From Theorem 1.1.1, we know that in the SIDH protocol, the first elliptic curve E_0 we work with is either maximal or minimal. Since isogenous curves have same cardinality [Feo, Theorem 13], all the curves computed as codomain of isogenies from E_0 are of the same type. The next theorem is the reason why we introduced this notion here.

Theorem 1.2.7. *[JKP+, Theorem 5.3] Let E a maximal elliptic curve over $\mathbb{F}_{p^2}$. If $\mathcal{A}$ is a maximal abelian variety of dimension $g \geq 2$ over $\mathbb{F}_{p^2}$, then $\mathcal{A}$ is isomorphic to E^g. The theorem holds if maximal is replaced by minimal.*

Therefore the 2-dimensional abelian varieties we will encounter in our analysis of SIDH will always split as a product of 2 elliptic curves. It matters for our *matrix representation* of isogenies between such abelian varieties. This is explained in Section 2.1.1.

1.3 How to break SIDH

We are still assuming that every isogeny we are working with is *separable*. Let us present two attacks on SIDH from respectively [MMP+] and [Rob]. They aim to solve the "Supersingular Isogeny with Torsion" problem (SSI-T), which is:

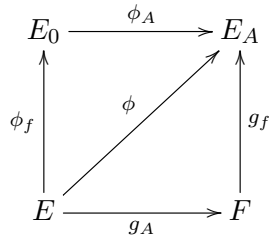
Problem. Let A and B be two coprime integers of roughly same size, and E_0, E_a two isogenous supersingular elliptic curves over a finite field $\mathbb{F}_{p^2}$, with p a prime not dividing A or B, linked by $\phi_A : E_0 \to E_a$ an isogeny of degree A. Knowing the action of ϕ_A on $E_0[B]$, compute ϕ_A.

The shared idea of Maino-Martindale's and Robert's attack is to construct an isogeny of abelian variety F, but in dimension greater than 1 (2 in the former, 8 in the later). Then we recover ϕ_A by evaluating F on some chosen points. Moreover F has a special form as an abelian variety: it is a product of isogenous maximal elliptic curves. That is why these products have a special status in this report.

1.3.1 Maino-Martindale's attack

The next theorem is at the heart of Maino-Martindale's attack. It is the theorem 1 of [MMP+], and relies on Kani's theorems [Kan1, Proposition 2.10, Corollary 2.11]. If the representation of an element of $Hom(E \times E_A, E_0 \times F)$ as a matrix of isogenies between elliptic curves is not clear, we encourage the reader to refer to Section 2.1.1.

Theorem 1.3.1. *Let $A = \ell_a^{e_a}$,$B = \ell_b^{e_b}$ where ℓ_a and ℓ_b are distinct primes, and $f = B - A > 0$. Assume that we have a commutative diagram between elliptic curves over $\mathbb{F}_{p^2}$,*



where the maps are isogenies such that $deg(\phi_f) = deg(g_f) = f$ and $deg(\phi') = deg(g_A) = N_a$.

Then the 2*-dimensional isogeny:*

$$F = \begin{pmatrix} \phi_f & -\widehat{\phi_A} \\ g_A & \widehat{g_f} \end{pmatrix} \in Hom(E \times E_A, E_0 \times F)$$

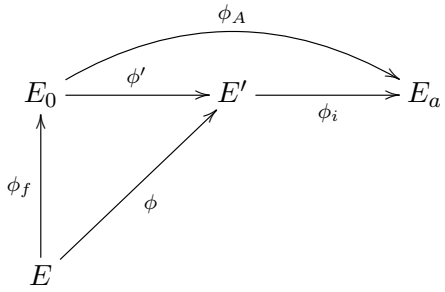
is a B*-isogeny with respect to the product polarization, and its kernel is:*

$$\mathrm{Ker}(F) = \{\big([A]P, \phi(P)\big) \mid P \in E[B]\} \simeq \big(\mathbb{Z}/B\mathbb{Z}\big)^2.$$

To attack SIDH, we have to compute an isogeny ϕ_f of fixed degree f. While it can be complicated to construct an isogeny of arbitrary degree, there is a class of isogenies for which this problem can be solved. These are isogenies of *smooth* degree. We give here a formal definition.

Definition 1.3.1. Let n be an integer. A $d \in \mathbb{Z}_{\geq 0}$ is called *n-smooth* if its prime factors are smaller than n.

If n is small enough, this notion is useful because we can efficiently factor an n-smooth integer. Here and subsequently we call d a *smooth* integer, if factoring it does not lead to too much computations. We have chosen to use this rather vague terminology because, in our context, deciding on the right n is a technical matter (see [MMP$^+$, Section 3.1]). What we are interested in is simply whether a smooth integer d can be factorised concretely, and thus a d-isogeny can be computed effectively [MMP$^+$, Section 3.2]. So the obstacle in our cryptanalysis is that f may not be smooth, and then it may be hard to effectively compute such a degree f isogeny. To mitigate this, we need to introduce several brute-force steps during the attack. We will twist f a little bit, to make it smooth. Following Maino-Martindale's article, we should keep in mind the following commutative diagram:



Where

- ϕ_A is the secret isogeny
- ϕ_f is an isogeny of degree f (during the algorithm, f is not exactly $B - A$, see **Step 1**.)
- ϕ_i is a guess for the last i steps of ϕ_A
- ϕ' represents the first $A - i$ corresponding steps
- ϕ is an $f\ell_a^{e_a - i}$-isogeny to which we want to apply Theorem 1.3.1

Let us describe the attack of [MMP$^+$], which aims at recovering ϕ_A.

Detail of the attack: We will denote by $\{P_b, Q_b\}$ (resp. $\{P_a, Q_a\}$) a basis of $E_0[B]$ (resp. of $E_0[A]$). We recall that we know $\phi_A(P_b)$ and $\phi_A(Q_b)$.

Step 1. We compute the parameters which lead to a smooth f:

- $0 \leq j \leq e_b$ and $0 \leq i \leq e_a$ with a small integer i.
- e a small and smooth integer such that $c = (A\ell_a^{-i})^{-1} \mod eB\ell_b^{-j}$.
- $f = eB\ell_b^{-j} - A\ell_a^{-i}$ is smooth and positive.

For simplicity of notation we write $A' = A\ell_a^{-i}$ and $B' = B\ell_b^{-j}$.

Step 2. We compute the associated f-isogeny.
We compute a curve E, f-isogenous to E_0, and an isogeny of degree f, $\phi_f : E \to E_0$, and we evaluate its dual on some points:

$$\widehat{\phi_f}(P_b), \widehat{\phi_f}(Q_b).$$

Step 3. Computation of a basis of $E[eB']$.
We compute such a basis $\{P_{eB'}, Q_{eB'}\}$, which satisfies:

$$\begin{aligned}[e]P_{eB'} =&[\ell_b^j]\widehat{\phi_f}(P_b)\\ [e]Q_{eB'} =&[\ell_b^j]\widehat{\phi_f}(Q_b)\end{aligned}$$

This is possible thanks to the surjectivity of the isogeny $[e]$.

Step 4. Beginning of the guess step.
We guess a $\phi_i : E' \to E_a$ for the last i steps of ϕ_A, and we choose $R, S \in E'[eB']$ such that:

$$\begin{aligned}[e]R =&[\ell_a^{-i} f \ell_b^j]\widehat{\phi_i} \circ \phi_A(P_b)\\ [e]S =&[\ell_a^{-i} f \ell_b^j]\widehat{\phi_i} \circ \phi_A(Q_b)\end{aligned}$$

In fact we hope that R (resp. S) corresponds to $\phi(P_{eB'})$ (resp. $\phi(Q_{eB'})$). A little computation shows that it is indeed a relation they have to satisfy.

Step 5. Computation of the 2-dimensional isogeny F_{guess}.
With this precautions we construct $K_{guess} = \langle \big(P_b, cR\big), \big(Q_b, cS\big)\rangle$, and the corresponding isogeny F_{guess}. There is an algorithm that checks if an abelian variety of dimension 2 splits as a product of elliptic curves [MMP$^+$, Remark 2]. We use it on the codomain of F_{guess}, to see if it factors through E_0. If it does not, we try with a new guess. In the other case (end of the guess step), we move on the next step. We denote F_{guess} by F.

Step 6. Evaluation of F.
We choose P, Q such that $\langle P, Q\rangle = E'[A']$, and we compute:

$$F(0, P) = \big(-\widehat{\phi'}(P), \widehat{g_f}(P)\big) \quad \text{and} \quad F(0, Q) = \big(-\widehat{\phi'}(Q), \widehat{g_f}(Q)\big)$$

The first component gives us the action of $\widehat{\phi}$ on the A'-torsion.

Step 7. Computation of ϕ_A.
By Remark 1.2.4 we recover the kernel of ϕ' which is an A'-isogeny, and then compute ϕ'. We are done, because $\phi_A = \phi_i \circ \phi'$.

1.3.2 Robert's attack

In this attack [Rob], we also want to have an f-isogeny which satisfies some good properties. But here, instead of twisting, we construct such an isogeny, but in dimension 4. The idea of using the matrix M as described below comes from the demonstration of a property called *Zarhin's trick*(see Theorem 13.12 of [Mil]). In the following, $f = B - A$.

Step 1. Construction of an f-isogeny.

A famous theorem due to Lagrange ([Sam, Section 5.7]) states that every positive integer is the sum of four squares.

$$f = f_1^2 + f_2^2 + f_3^2 + f_4^2 \quad with \quad f_1,\, f_2,\, f_3,\, f_4 \in \mathbb{Z}_{\geq 0}.$$

Let $M \in \mathcal{M}_4(\mathbb{Z})$ denote the matrix of the multiplication by $f_1+f_2i+f_3j+f_4k$ in the non-commutative quaternion algebra $\mathbb{Z}[i,j,k]$, where: $i^2 = j^2 = k^2 = ijk = -1$. Let us denote by $\phi_f \in End(E_0^4)$ the endomorphism represented by M. With Proposition 2.1.1, we see that $\widetilde{\phi_f}$ is represented by M^t, since the isogenies $[n]$ are self dual. Moreover a straightforward computation leads to:

$$MM^t = fI_4.$$

So we have

$$\phi_f \widetilde{\phi_f} = fId_{E_0^4}$$

and then ϕ is a 4-dimensional f-isogeny.

Step 2. Construction of a B-isogeny.

Let α denote the endomorphism represented by M, but on E_a^4 this time. We also write $\phi_A I_4 : E_0^4 \to E_a^4$ for the diagonal isogeny induced by ϕ_A. Since ϕ_f and α are integer matrices, they commute with all the other isogenies. This gives us the following commutative diagram:

$$\begin{array}{ccc} E_0^4 & \xrightarrow{\phi_A I_4} & E_a^4 \\ {\scriptstyle \phi_f}\downarrow & & \downarrow{\scriptstyle \alpha} \\ E_0^4 & \xrightarrow[\phi_A I_4]{} & E_a^4 \end{array}$$

Thus we construct the 8-dimensional endomorphism component-wise on $X = E_0^4 \times E_a^4$:

$$F = \begin{pmatrix} \phi_f & \widetilde{\phi_A} I_4 \\ -\phi_A I_4 & \tilde{\alpha} \end{pmatrix}.$$

Then by Proposition 2.1.1:

$$\tilde{F} = \begin{pmatrix} \widetilde{\phi_f} & -\widetilde{\phi_A} I_4 \\ \phi_A I_4 & \alpha \end{pmatrix}.$$

A quick computation leads to:

$$F\tilde{F} = \tilde{F}F = (A + f)Id_X = BId_X.$$

Thus F is a B-isogeny on X, with respect to the product polarizations.

Step 3. Computing the kernel of F.

We know that F is a B-isogeny on X, so by Remark 1.2.4 $\mathrm{Ker}(F) = \tilde{F}(X[B])$, but we need to be more accurate.

Claim. Let us denote $S = \{(\tilde{\phi_f}(P),\, \phi_A I_4(P) \mid P \in E_0^4[B]\}$. Then

$$\mathrm{Ker}(F) = S = \tilde{F}\big(E_0^4[B] \times 0\big).$$

Proof. The second equality is obvious, we focus on the first one. With the above remark, we already have

$$S = \tilde{F}\big(E_0^4[B] \times 0\big) \subset \tilde{F}(X[B]) = \mathrm{Ker}(F).$$

Hence $S \subset \mathrm{Ker}(F)$. But we also have $\mathrm{Ker}(\tilde{\phi_f}) \subset E_0^4[f]$ and $\mathrm{Ker}(\phi_A\, I_4) \subset E_0^4[A]$ because they are respectively f and A isogenies. Since f and A are coprime:

$$\mathrm{Ker}(\widetilde{\phi_f}) \cap \mathrm{Ker}(\phi_A I_4) = \{0\}.$$

Thereby $\mathrm{Card}(S) = \mathrm{Card}(E_0^4[B])$, because the map $P \mapsto \big(\widetilde{\phi_f}(P),\, \phi_A I_4(P)\big)$ is injective on $E_0^4[B]$. That is why:

$$\mathrm{Card}(S) = \mathrm{Card}(E_0^4[B]) = B^{2\times dim(E_0^4)} = B^8$$

It remains to show that $\mathrm{Card}(\mathrm{Ker}(F)) = B^8$. We know that $[B] = F \circ \tilde{F}$, equality holding between 8-dimensional isogenies. Hence taking their degree (Theorem 1.2.1 for $\deg([B])$)

$$B^{2*8} = \deg(F)\deg(\tilde{F}) = \deg(F)^2 = \mathrm{Card}(\mathrm{Ker}(F))^2$$

And finally $\mathrm{Card}(\mathrm{Ker}(F)) = B^8$. □

We made a big step by introducing S, because we can compute it. Indeed, we know ϕ_f and the action of ϕ_A on $E_0[B]$.

Step 4. Obtaining critical parameters.

We assume that there is a way to, knowing an abelian variety X and an isogeny F with kernel $\mathrm{Ker}(F) \subset X$, compute a rational expression of F (see [LR]). Thus we can evaluate F on suitable points of X. Especially, if $\{Q_1, Q_2\}$ is a basis of $E_a[A]$ (E_a is transmitted by Alice during the protocol, and A is not secret), then we can compute $\widetilde{\phi_A}(Q_i)$ by evaluating F on $(0,0,0,0,Q_i,0,0,0) \in E_0^4 \times E_a^4$. Once again, by Remark 1.2.4, we can recover the kernel of ϕ_A, and compute this secret isogeny.

1.4 M-SIDH countermeasure, masking the torsion points

1.4.1 M-SIDH protocol

In cryptography when a protocol is broken, we often try to patch the flaw. The work of [FMP], M-SIDH, is the perfect example where we upgrade the SIDH protocol, in order to make it resistant against the previous attacks. First we recall some notations.

Definition 1.4.1. For $N \geq 2$ integer, let us denote:

$$\mu_2(N) = \{x \in \mathbb{Z}/N\mathbb{Z} \mid x^2 = 1 \mod N\}$$

In the notation of Section 1.1.1, we fix $p = AB - 1$ a prime number, A and B coprime integers, such that $E_0(\mathbb{F}_{p^2}) = \Big(\mathbb{Z}/(p+1)\mathbb{Z}\Big)^2$. However now A and B are smooth. We also keep the notations: $E_0[A] = \langle P_a, Q_a\rangle$ and $E_0[B] = \langle P_b, Q_b\rangle$. Let us describe the protocol.

Private Settings
Alice randomly chooses $x_a \in \mu_2(B)$ and $s_a \in \mathbb{Z}/A\mathbb{Z}$. Then she computes $\phi_A : E_0 \to E_a$, where $E_a = E_0/\langle P_a + [s_a]Q_a\rangle$, and the keys:

- public: $\big(E_a, [x_a]\phi_A(P_b), [x_a]\phi_A(Q_b)\big)$
- private: s_a

And she finally forgets x_a.

Symmetrically Bob randomly chooses $x_b \in \mu_2(A)$ and $s_b \in \mathbb{Z}/B\mathbb{Z}$. Then he computes $\phi_B : E_0 \to E_b$, where $E_b = E_0/\langle P_b + [s_b]Q_b\rangle$, and the keys:

- public: $\big(E_b, [x_b]\phi_B(P_a), [x_b]\phi_B(Q_a)\big)$
- private: s_b

And he finally forgets x_b.

Exchange
Alice sends her public key to Bob, which will be denoted by $\big(E_a, R_b, S_b\big)$.
Bob sends his public key to Alice, which will be denoted by $\big(E_b, R_a, S_a\big)$.

Computation of shared key
We will only describe the procedure followed by Alice, Bob's one being symmetrical. Alice received $\big(E_b, R_a, S_a\big)$. First she does a safety test: $e_a(R_a, S_a) = e_a(P_a, Q_a)^B$. Indeed if she well received Bob's key, we check that:

$$\begin{aligned} e_a(R_a, S_a) &= e_a\big([x_b]\phi_B(P_a), [x_b]\phi_B(Q_a)\big) \\ &= [x_b^2]\, e_a\big(\phi_B(P_a), \phi_B(Q_a)\big) \\ &= e_a\big(\phi_B(P_a), \phi_B(Q_a)\big) \\ &= e_a(P_a, Q_a)^{\deg(\phi_B)} = e_a(P_a, Q_a)^B. \end{aligned}$$

If the equality fails, Alice stops the procedure. Otherwise she computes the shared key:

$$E_{ba} = E_b \,/\, \langle R_a + [s_a]S_a\rangle.$$

Bob also checks if $e_b(R_b, S_b) = e_b(P_b, Q_b)^A$, e_b being the B-Weil pairing on E_b. If it holds he computes the shared key:

$$E_{ab} = E_a \,/\, \langle R_b + [s_b]S_b\rangle.$$

Let us check that E_{ab} and E_{ba} have the same j-invariant.

$$\begin{aligned} E_{ba} &\simeq E_b \,/\, \langle R_a + [s_a]S_a \rangle \\ &\simeq E_b \,/\, \langle [x_b]\phi_B(P_a) + [s_a][x_b]\phi_B(Q_a) \rangle \\ &\simeq E_b \,/\, \langle \phi_B\big([x_b]P_a + [s_a][x_b]Q_a\big) \rangle \\ &\simeq E \,/\, \langle \big(P_b + [s_b]Q_b\big), \big([x_b]P_a + [s_a][x_b]Q_a\big) \rangle \end{aligned}$$

But $x_b \in \mu_2(A)$ is invertible, so we have $\langle [x_b]\big(P_a + [s_a]Q_a\big) \rangle = \langle \big(P_a + [s_a]Q_a\big) \rangle$. And then:

$$E_{ba} \simeq E_0 \,/\, \langle \big(P_b + [s_b]Q_b\big), \big(P_a + [s_a]Q_a\big) \rangle.$$

The same proof works for E_{ab}, we conclude that

$$E_{ab} \simeq E_0 \,/\, \langle \big(P_b + [s_b]Q_b\big), \big(P_a + [s_a]Q_a\big) \rangle \simeq E_{ba}.$$

The j-invariant is then the shared secret.

1.4.2 Why the previous attack no longer work

What happens if we try to use Robert's attack on M-SIDH? Since A and B are still known, we can construct the matrix $M \in \mathcal{M}_4(\mathbb{Z})$ given by the decomposition of $f := B - A$ as a sum of 4 squares. We can also still compute two f-isogenies, $\phi_f : E_0^4 \to E_0^4$ and $\alpha : E_a^4 \to E_a^4$, such that the following diagram commutes.

$$\begin{array}{ccc} E_0^4 & \xrightarrow{\phi_A I_4} & E_a^4 \\ {\scriptstyle \phi_f}\downarrow & & \downarrow{\scriptstyle \alpha} \\ E_0^4 & \xrightarrow[\phi_A I_4]{} & E_a^4 \end{array}$$

The main difference is that the following set, constructed by Robert in his attack,

$$\{(\widetilde{\phi_f}(P),\, \phi_A I_4(P) \mid P \in E_0^4[B]\}$$

is no longer accessible, because we do not know the action of ϕ_A on the B-torsion. So we naturally replace it by:

$$S := \{(\widetilde{\phi_f}(P),\, [x_b]\phi_A I_4(P) \mid P \in E_0^4[B]\}.$$

We have two options so far, we can either continue the attack, or virtually introduce a twist by $[x_b]$ in the previous diagram.

First possibility
First, we try without modifying the attack. Thus we define

$$F = \begin{pmatrix} \phi_f & \widetilde{\phi_A} I_4 \\ -\phi_A I_4 & \tilde{\alpha} \end{pmatrix}$$

with its dual, as in the **step 2** of Robert's attack. So we have theoretically a B-isogeny, but we do not know anything on its kernel. Indeed now we have $[x_b]$ in the definition of S which breaks the link between S and $\mathrm{Ker}(F)$:

$$F \begin{pmatrix} \widetilde{\phi_f}(P) \\ [x_b]\phi_A I_4(P) \end{pmatrix} = \begin{pmatrix} (f + x_b A).P \\ -\phi_A I_4 \widetilde{\phi_f}(P) + \tilde{\alpha}[x_b]\phi_A I_4(P) \end{pmatrix} \quad \left(\neq \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad \text{generally speaking} \right)$$

That is why we can no longer evaluate F on chosen points, to find critical parameters.

Second possibility
If we modify the diagram as we did for S we have:

$$\begin{array}{ccc} E_0^4 & \xrightarrow{[x_b]\phi_A I_4} & E_a^4 \\ {\scriptstyle \phi_f}\downarrow & & \downarrow{\scriptstyle \alpha} \\ E_0^4 & \xrightarrow[[x_b]\phi_A I_4]{} & E_a^4 \end{array}$$

which is still commutative because we only use the endomorphism $[x_b]$ which commutes with all isogenies. Here we have another isogeny on $E_0^4 \times E_a^4$ given by:

$$F = \begin{pmatrix} \phi_f & [x_b]\widetilde{\phi_A} I_4 \\ -[x_b]\phi_A I_4 & \tilde{\alpha} \end{pmatrix}$$

One checks that F is an $f + x_b^2 A$-isogeny. But we have

$$f + x_b^2 A = B(1 + A\frac{x_b^2 - 1}{B})$$

So S cannot be the kernel of F, because it has too many points (except in the case of $x_b = \pm 1$, which has to be excluded). Therefore F factors through an isogeny of degree B and an isogeny of degree $1 + A\frac{x_b^2-1}{B}$. The last degree may not be smooth and is greater than A, so it is not possible to effectively recover the factors of F. We conclude that we cannot evaluate F this way.

This explains why M-SIDH might be a good successor to SIDH, and today there is no known effective attack. However it is clear that matrices of isogenies play a central role in the cryptosystem. That is why we decided to look at them.

2 Computation of isogenies between maximal abelian surfaces

In our analysis of M-SIDH, it is essential to compute isogenies between products of two elliptic curves from their kernel. We will call these products of elliptic curves *product surfaces*. This chapter focuses on the computation of isogenies between such surfaces, with both theoretical and practical results.

2.1 Representation

We continue to assume that every isogeny we are working with is *separable*.

2.1.1 Matrix of isogenies

The software MAGMA [BCP] provides powerful functions for computing isogenies of elliptic curves. However there is no implementation of higher dimension abelian varieties, nor isogenies between them. Here we explain a method to deal with these objects. We can represent a product of elliptic curves $E_1 \times \cdots \times E_n$ with the Cartesian product in MAGMA. Nevertheless this loses the algebraic structure, since MAGMA gives the product of the underlying set without equipping it with the component-wise group law. Since isogenies are group morphisms, we need to find a way to deal with these objects. Our method is based on the following isomorphism. Let $A := A_1 \times \cdots \times A_n$ and $A' := A'_1 \times \cdots \times A'_m$ be products of abelian varieties over the same field k, then there is an isomorphism of k-algebras: ([Kan2, §4.1])

$$T_{A,A'} : \mathrm{Hom}_k(A, A') \xrightarrow{\sim} \bigoplus_{i=1}^{m} \bigoplus_{j=1}^{n} \mathrm{Hom}_k(A_j, A'_i)$$

which respects the composition of k-morphisms. This means that if $A'' := A''_1 \times \cdots \times A''_r$ is another product of abelian varieties, then:

$$T_{A,A''}(f' \circ f) = T_{A',A''}(f') \cdot T_{A,A'}(f)$$

for $f \in \mathrm{Hom}(A, A')$, $f' \in \mathrm{Hom}(A', A'')$, and where $\cdot$ is the usual matrices multiplication.

In our case $A = E_1 \times E_2$ and $A' = E'_1 \times E'_2$ where E_i and E'_j are elliptic curves over a finite field. Thus a matrix $\begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix}$ (implemented as the list $[f_{11}, f_{12}, f_{21}, f_{22}]$) of 4 isogenies $f_{ij} : E_j \to E'_i$ represents 2-dimensional morphisms, moreover *all* 2-dimensional isogenies can be represented this way, if we allow some of the f_{ij} to be zero.

In Chapter 1 we saw the construction of the adjoint isogeny with respect to polarization, which we denoted $\widetilde{f}$. The following proposition explains how it interacts with the Cartesian product, if we represent isogenies as matrices.

Proposition 2.1.1. *[Rob, Lemma 3.2] For $i \in \{1, \dots, 4\}$, let $\mathcal{A}_i$ denote an abelian variety and $\lambda_i : \mathcal{A}_i \to \widehat{\mathcal{A}_i}$ a polarization. If $\Phi : \mathcal{A}_1 \times \mathcal{A}_2 \to \mathcal{A}_3 \times \mathcal{A}_4$ is an isogeny represented by the matrix of isogenies: $\begin{pmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{pmatrix}$ then we have:*

$$\widetilde{\Phi} = \begin{pmatrix} \widetilde{f_{11}} & \widetilde{f_{21}} \\ \widetilde{f_{12}} & \widetilde{f_{22}} \end{pmatrix}$$

for the product polarization.

2.1.2 Brute-force research from kernel

The aim of the algorithm

Let us summarize what we want. We fix ℓ a prime, two isogenous supersingular elliptic curves E_1, E_2 over a finite field $\mathbb{F}_{p^2}$ such that the ℓ-torsion is rational. Now, given $P, Q \in (E_1 \times E_2)[\ell]$ $\mathbb{Z}$-linearly independent, we want to find morphisms $f_{11}, f_{12}, f_{21}, f_{22}$ where $\text{Domain}(f_{ij}) = E_i$, such that the 2-dimensional isogeny represented by (f_{ij}) has kernel $K := \langle P, Q \rangle$. Our hope is that it may exist such a matrix (f_{ij}), with $d_{ij} := \deg(f_{ij})$ not too large compared to ℓ.

Remark 2.1.1. Notice that in M-SIDH, the elliptic curve E_0 is *maximal* and never minimal. The following work is valid for both maximal and minimal abelian varieties, but to simplify notation we only state the properties for the maximal case.

First, we have to be sure that this matrix exists. More precisely, given a finite subgroup $K \subset E_1 \times E_2$ and an isogeny F with kernel K, the codomain of F must be isomorphic to a product surface. This is why we have introduced the notion of *maximal abelian variety*. Indeed Theorem 1.2.7 tells us that such an abelian variety of dimension 2 over $\mathbb{F}_{p^2}$ is isomorphic to a product of elliptic curves. Thus given a finite subgroup K of $E_1 \times E_2$ where E_1 and E_2 are maximal over $\mathbb{F}_{p^2}$, there exists an isogeny with codomain a product surface $E_1' \times E_2'$ and kernel K. Moreover the previous theorem states that the E_i' are also maximal. We can therefore perpetuate the process with $K' \subset E_1' \times E_2'$ and so on, which is crucial for the next paragraph.

One might think that this assumption (maximal or minimal over $\mathbb{F}_p^2$) is too restrictive, but in practice we always work within this framework. Indeed the elliptic curves $E_0,\ E_a,\ E_b$ in SIDH and M-SIDH are maximal (or minimal in SIDH), see Theorem 1.1.1.

Remark 2.1.2. Another theorem by Kani could have been invoked. We can find in [Kan2, Theorem 2] that if an abelian variety $\mathcal{A}$ is isogenous to a product E^n, where E is a CM elliptic curve, then there exist elliptic curves $E_1, ..., E_n$ such that $\mathcal{A} \simeq E_1 \times ... \times E_n$. Now an elliptic curve on a finite field is always CM because of the Frobenius endomorphism, so the theorem holds here. We have chosen to speak of maximal abelian varieties because under this condition, which is true in our cryptographic applications, we get a stronger result. Indeed Theorem 1.2.7 tells us that there is only *one* isomorphism class for each dimension.

Now we explain how we go from an algorithm that finds the matrix of isogenies only for a kernel in a prime torsion, to a protocol that works for any composed B-torsion. Consequently our algorithm only has to deal with the case of prime torsion. This is a general construction of composed degree isogenies. For instance, let $B = \ell_1\ell_2$, with ℓ_i prime numbers, and $K = \langle P, Q\rangle \subset (E_1 \times E_2)[B]$. We denote $B' = B/\ell_1$ and $K_{\ell_1} = B' \cdot K = \langle B' \cdot P, B' \cdot Q\rangle$. Note that if K is maximal isotropic for the B-Weil pairing, then K_{ℓ_1} is maximal isotropic for the ℓ_1-Weil pairing. We can define $F_1 : E_1 \times E_2 \to E_1' \times E_2'$ the 2-dimensional isogeny with kernel K_{ℓ_1}, given by our algorithm because $K_{\ell_1} \subset (E_1 \times E_2)[\ell_1]$. The codomain of F_1 splits thanks to the previous paragraph. If we denote by K' the group $F_1(K)$, then K' is in the ℓ_2-torsion of a product surface $E_1' \times E_2'$, and our algorithm finds an other isogeny of product surfaces F_2 with kernel K'. It follows that the composition $F_2 \circ F_1$ has kernel exactly K.

$$E_1 \times E_2 \xrightarrow[\mathrm{Ker}(F_1)=K_{\ell_1}]{} E_1' \times E_2' \xrightarrow[\mathrm{Ker}(F_2)=F_1(K)=K']{} E_1'' \times E_2'' \qquad \mathrm{Ker}(F_2 \circ F_1) = K$$

If B' is not prime, we repeat the process with $B'' = B'/\ell'$ where ℓ' is a prime factor of B', and call our algorithm on $B'' \cdot K'$ which is in the ℓ'-torsion, and so on.

Details of the implementation

Our approach is to find a solution by brute-forcing, *i.e.* to test every combinations of f_{ij} by increasing the maximum degree of the 1-dimensional isogenies in the matrix. Our algorithm is based on a main loop, on the maximum degree of the isogenies in the matrix we are looking for. So we start with this maximum degree $S = 2$ and at the end of our process, if no isogeny is found, we try again after incrementing S. Here are the main steps of a loop.

Steps of the algorithm

Step 1. Computation of candidate j-invariants.

The following function computes the j-invariants of curves E', such that there is an isogeny $\varphi : E \to E'$ with $\#\mathrm{Ker}(\varphi) < S$ and $\mathrm{Ker}(\varphi) = \langle P\rangle$ for a point $P \in E$. We call these: *cyclic isogenies*.

```
function cyclic_isogeny_neighbours(E, S)
/* Computes the j-invariants of all curves connected to E via a cyclic S isogeny */
    k := BaseRing(E);
    assert S gt 1;
    degext := LCM([1] cat [Degree(f[1])
                           : f in Factorization(DivisionPolynomial(E, S))]);
    K := ext<k | degext>;
    E2 := BaseChange(E, K);
    division_points := Points(TorsionSubgroupScheme(E2, S));
    res := {k!jInvariant(F)
            where F, _ is IsogenyFromKernel(SubgroupSchemeFromGenerators(E2, P))
            : P in division_points | Order(P) eq S};
    return res;
end function;
```

This function is used with the parameters (E_1, S) and (E_2, S), to obtain pairs of j-invariants (j_1, j_2). Those pairs represent isomorphism classes of possible codomains for the matrix we are looking for.

Step 2. Beginning of the loop on the possible degrees.

In this section we have no information about the final matrix. It can have null morphisms and it may be diagonal, upper or lower triangular. So for each list of degree $[d_{ij}]$ we have to check all possible pairs of j-invariant for each of these cases, which slows down our algorithm a lot.

```
for degs in { ls : ld in CartesianPower({1..S}, 4)
              | Max(ls) eq S  and
              /* Avoid permutations of rows */
             ((ls[1] lt ls[3]) or (ls[1] eq ls[3] and ls[2] le ls[4]))
              where ls is [ld[i] : i in [1..4]] } do

        candidates_jFullMatrix := {[a, b] : a in candidates_j_1[degs[1]],
                                            b in candidates_j_1[degs[3]]
                                  | a in candidates_j_2[degs[2]] and
                                    b in candidates_j_2[degs[4]] };

        candidates_jUpperMatrix := {[a, b] : a in candidates_j_1[degs[1]],
                                             b in candidates_j_2[degs[4]]
                                  | a in candidates_j_2[degs[2]] };

        candidates_jLowerMatrix := {[a, b] : a in candidates_j_1[degs[1]],
                                             b in candidates_j_1[degs[3]]
                                  |  b in candidates_j_2[degs[4]] };

        candidates_jDiagMatrix := {[a, b] : a in candidates_j_1[degs[1]],
                                            b in candidates_j_2[degs[4]]};

        if IsEmpty(candidates_jDiagMatrix) then continue; end if;
```

Step 3. Beginning of the loop on the pairs of j-invariants.

This is the main step, but we will not go into detail here. For each pair of j-invariants and each type of matrix (full, diagonal, upper or lower triangular) we construct all the isogenies of desired degree. The following figure shows how to do this when the isogenies have cyclic kernels, but our algorithm can also handle the general case.

```
for i in L_iToTest do
    if degsP[i] eq 1 then
        if IsIsomorphic(Es[i],EllipticCurveFromjInvariant(k!jjs[i])) then
            isogsP cat:=[IsomorphismToIsogeny(
                    Isomorphism(Es[i],EllipticCurveFromjInvariant(k!jjs[i])))];
        else
            break n4;
        end if;
    else

    tlist := { T : T in division_points[i]
              |#{j*T: j in [1..degsP[i]]} eq degsP[i]
              and jFromGeneratedP(Eext[i],T,degsP[i]) eq K!jjs[i] };

    if IsEmpty(tlist) then
        break n4;
    end if;

    candidates_kernel := Random(tlist);
    pol_kernel := &*{PolynomialRing(K).1 - (n*Eext[i]!candidates_kernel)[1]
                        : n in [1..degsP[i]-1]};
    if not &and[c^#k eq c : c in Eltseq(pol_kernel)] then
        flag_continue := true;
        break i;
    end if;
    isogsP cat:= [phi where _, phi is
          IsogenyFromKernel(SubgroupScheme(Es[i], PolynomialRing(k)!pol_kernel))];
    end if;
end for;

if flag_continue then
    continue jj;
end if;
```

Step 4. Testing all the possible quadruplets of isogenies.

In this last step we check if the bound S on the degrees of the 1-dimensional isogenies leads to a result. We have to perform several tests, depending on the type of matrix we are looking for. These tests look like the following:

```
 isogs:=[ MultiplicationByMMap(Domain(isogsP[i]),ni[i]) * isogsP[i] : i in [1..4] ];
 phi1 := Isomorphism(Codomain(isogs[1]), Codomain(isogs[2]));
 phi2 := Isomorphism(Codomain(isogs[3]), Codomain(isogs[4]));

```

```
5  /* if the Matrix is full */
6
7      if phi1(isogs[1](Eext[1]![P[1][i] : i in [1..3]])) eq
8         -isogs[2](Eext[2]![P[2][i] : i in [1..3]])
9
10     and phi2(isogs[3](Eext[1]![P[1][i] : i in [1..3]])) eq
11        -isogs[4](Eext[2]![P[2][i] : i in  [1..3]])
12
13     and phi1(isogs[1](Eext[1]![Q[1][i] : i in [1..3]])) eq
14        -isogs[2](Eext[2]![Q[2][i] : i in [1..3]])
15
16     and phi2(isogs[3](Eext[1]![Q[1][i] : i in [1..3]])) eq
17        -isogs[4](Eext[2]![Q[2][i] : i in [1..3]])
18
19     then
20
21     return <isogs, phi1, phi2>;
```

We check that the matrix vanishes on $\{P, Q\}$, then we return the result. In the other case, we increment S and we restart at **Step 1**. We know that this algorithm ends, but it is very slow. The next section aims at speeding up this algorithm.

2.2 Maximal isotropic kernels

2.2.1 Theoretical contributions

We quickly ran into practical problems, there is too many combinations to test naively. So we want effective conditions on the f_{ij} to reduce the number of tests. The propositions of this section aim to meet this need, but we had to restrict ourselves to one particular case, the case where K is *maximal isotropic* (see Definition 1.2.9). We fix E_1, E_2 two maximal isogenous elliptic curves over a finite field $\mathbb{F}_{p^2}$ with their respective canonical polarizations λ_1, λ_2. We also fix a prime number ℓ (coprime to p) such that the ℓ-torsion subgroups of E_1 and E_2 are rational. We start with a special case for which it is easy to find a matrix representation.

Definition 2.2.1. Let K be a maximal isotropic subgroup of the product surface $E_1 \times E_2$ for $e_\ell^{\lambda_1 \otimes \lambda_2}$. We call K *diagonal*, if for all $(P_1, P_2), (Q_1, Q_2) \in K$ we have:

$$e_{E_1,\ell}(P_1, Q_1) = 1 \quad \textit{and} \quad e_{E_2,\ell}(P_2, Q_2) = 1$$

The following proposition gives us the representation of an isogeny having a diagonal kernel.

Proposition 2.2.1. *Let $K \subset (E_1 \times E_2)[\ell]$ be a diagonal subgroup, we fix $\{(P_1, P_2), (Q_1, Q_2)\}$ a basis of K as a free $(\mathbb{Z}/\ell\mathbb{Z})$-module of rank 2. Then there are isogenies $\phi_i : E_i \to E_i'$ such that the 2-dimensional isogeny*

$$\begin{array}{rccc} F : E_1 \times E_2 & \to & E_1' \times E_2' \\ (T_1, T_2) & \mapsto & (\phi_1(T_1), \phi_2(T_2)) \end{array}$$

satisfies $\mathrm{Ker}(F) = K$.

Proof. Since K is diagonal we know that P_1 and Q_1 (resp. P_2 and Q_2) are $\mathbb{Z}$-linearly dependent. Without loss of generality we can assume that $Q_1 \in \langle P_1 \rangle$ (resp. $Q_2 \in \langle P_2 \rangle$) with P_1 (resp. P_2) of order ℓ. Thus for $i \in \{1,2\}$, $\langle P_i, Q_i \rangle = \langle P_i \rangle$. Let us denote by $\phi_i : E_i \to E_i'$ one isogeny with kernel $\langle P_i \rangle$, so that we obtain

$$\begin{aligned}(T_1,T_2) \in K &\iff \exists\ \lambda_1,\lambda_2 \in \mathbb{F}_{p^2} \mid (T_1,T_2) = \lambda_1 \cdot (P_1,P_2) + \lambda_2 \cdot (Q_1,Q_2)\\ &\iff T_1 \in \langle P_1, Q_1 \rangle \text{ and } T_2 \in \langle P_2, Q_2 \rangle\\ &\iff T_1 \in \langle P_1 \rangle \text{ and } T_2 \in \langle P_2 \rangle\\ &\iff T_1 \in \mathrm{Ker}(\phi_1) \text{ and } T_2 \in \mathrm{Ker}(\phi_2)\end{aligned}$$

And since ϕ_1 and ϕ_2 are surjective and group morphisms, so is F. Consequently F is an isogeny (its kernel K is finite). □

This proposition is effective, since we can compute F. Indeed, if MAGMA computes ϕ_i with Vélu's formula then F is represented by $\begin{pmatrix}\phi_1 & 0\\ 0 & \phi_2\end{pmatrix}$. With this observation it is easy to compute an isogeny between product surfaces whose kernel is diagonal. The hardest part is for non-diagonal maximal isotropic subgroups.

Remark 2.2.1. Thanks to Remark 1.2.5, if $K = \langle (P_1,P_2),(Q_1,Q_2) \rangle$ is a non-diagonal maximal isotropic subgroup of $E_1 \times E_2$ for $e_\ell^{\lambda_1 \otimes \lambda_2}$, then $\{P_1, Q_1\}$ (resp. $\{P_2, Q_2\}$) forms a $\mathbb{Z}$-basis of $E_1[\ell]$ (resp. $E_2[\ell]$).

Here and subsequently $K = \langle P, Q \rangle$ stands for such a non-diagonal isotropic maximal subgroup of $E_1 \times E_2$ for $e_\ell^{\lambda_1 \otimes \lambda_2}$, if nothing else is specified. In that case we proved that an isogeny F whose kernel is K is represented by a matrix of non-zero morphisms. First we need a lemma which is *Corollary 64* in [Kan3].

Lemma 2.2.1. *Let $F : E_1 \times E_2 \to E_1' \times E_2'$ be an isogeny represented by the matrix $(f_{ij})_{i,j\in\{1,2\}}$. If f_{21} is the null-morphism, then:*

$$\deg(F) = d_{11}d_{22}.$$

Proof. Following the proof of Kani's corollary, we can show that if $f_{21} \equiv 0$ then:

$$\deg(F) = |d_{11}(d_{12}+d_{22}) - \deg(\widehat{f_{12}} \circ f_{11})|$$

which leads to $\deg(F) = d_{11}d_{22}$. □

Proposition 2.2.2. *Let $F : E_1 \times E_2 \to E_1' \times E_2'$ be an isogeny of kernel K, represented by the matrix $(f_{ij})_{i,j\in\{1,2\}}$. Then the f_{ij} are non-zero morphisms.*

Proof. Let us assume that $f_{21} \equiv 0$ (We only do one case, the others are similar). Then for all $(T_1,T_2) \in K$ we have $f_{22}(T_2) = 0_{E_2'}$, but K is non-diagonal and maximal isotropic so $E_2[\ell] \subset \mathrm{Ker} f_{22}$ and hence $\ell^2 | d_{22}$. By application of the previous lemma, we have:

$$\ell^2 = d_{11}d_{22}.$$

Consequently $d_{11} = 1$ and $d_{22} = \ell^2$. That is why we can represent F by $\begin{pmatrix} \phi_1 & f_{12} \\ 0 & [\ell] \circ \phi_2 \end{pmatrix}$ where the $\phi_j : E_j \to E'_j$ are isomorphisms. Then by Proposition 2.1.1 we have, $\tilde{F} = \begin{pmatrix} \phi_1^{-1} & 0 \\ \widehat{f_{12}} & [\ell] \circ \phi_2^{-1} \end{pmatrix}$. But by duality $\#\mathrm{Ker}(F) = \#\mathrm{Ker}(\tilde{F})$, and then for $(P, Q) \in \mathrm{Ker}(\tilde{F})$ not trivial we have: $\phi_1^{-1}(P) = 0$, which is absurd since ϕ_1^{-1} is an isomorphism. □

Therefore, when we are dealing with maximal isotropic subgroups, we do not need to check every possible types of matrices. We only need to check if K is diagonal, and if it is not, we know that it is associated with a matrix without 0. Thus the degrees of the isogenies composing the matrix are well defined, and we can give a necessary condition on these degrees.

Proposition 2.2.3. *Let $F : E_1 \times E_2 \to E'_1 \times E'_2$ be an isogeny of kernel K, represented by the matrix $(f_{ij})_{i,j\in\{1,2\}}$. Let us denote by d_{ij} the degree of f_{ij}, then:*

$$d_{11} + d_{12} \equiv 0 \bmod \ell$$
$$d_{21} + d_{22} \equiv 0 \bmod \ell$$

Proof. Let $i \in \{1, 2\}$ represent the row we are studying. Throughout the proof, e_j (resp. e'_j) denotes the ℓ-Weil pairing on E_j (resp. E'_j). Thanks to the previous remark, $\langle P_i, Q_i \rangle = E_i[\ell]$. Since P is in the kernel of F, $f_{i1}(P_1) + f_{i2}(P_2) = 0_{E'_i}$. Then for all $Q \in E'_i[\ell]$ we have:

$$\begin{aligned} 1 =& e'_i(f_{i1}(P_1) + f_{i2}(P_2), Q) \\ =& e'_i(f_{i1}(P_1), Q) \cdot e'_i(f_{i2}(P_2), Q) \end{aligned}$$

Hence for $Q = f_{i1}(Q_1)$:

$$\begin{aligned} 1 =& e'_i(f_{i1}(P_1), f_{i1}(Q_1)) \cdot e'_i(f_{i2}(P_2), f_{i1}(Q_1)) \\ =& e_1(P_1, Q_1)^{d_{i1}} \cdot e'_i(f_{i2}(P_2), f_{i1}(Q_1)) \end{aligned}$$

But Q is in the kernel of F, so: $f_{i1}(Q_1) = f_{i2}(-Q_2)$. Therefore:

$$\begin{aligned} 1 =& e_1(P_1, Q_1)^{d_{i1}} \cdot e'_i(f_{i2}(P_2), f_{i1}(Q_1)) \\ =& e_1(P_1, Q_1)^{d_{i1}} \cdot e'_i(f_{i2}(P_2), f_{i2}(-Q_2)) \\ =& e_1(P_1, Q_1)^{d_{i1}} \cdot e_2(P_2, -Q_2)^{d_{i2}} \end{aligned}$$

and finally:

$$e_1(P_1, Q_1)^{d_{i1}} = e_2(P_2, Q_2)^{d_{i2}}. \tag{2.1}$$

We know that $e_1(P_1, Q_1) = e_2(P_2, Q_2)^{-1}$ because K is maximal isotropic, then:

$$e_1(P_1, Q_1)^{d_{i1}+d_{i2}} = 1.$$

Moreover $e_1(P_1, Q_1) \neq 1$ because K is not diagonal, and we can conclude: $d_{i1} + d_{i2} \equiv 0 \bmod \ell$. □

2.2.2 The polarized algorithm

We have seen the general algorithm, but it is very slow and we do not know how to speed it up at the moment. In this part we will assume that the kernels have an additional property, namely that they are *maximal isotropic* for the product polarization. With this additional assumption, we can increase the performance of our algorithm, thanks to the results of Section 2.2.1. We specialize in this case because it appears in M-SIDH. Indeed in this context we see that if $\phi_a : E_0 \to E_a$ is the secret A-isogeny, and $\phi_f : E_0 \to E_f$ an f-isogeny we choose, then the subgroup:

$$G := \{\big(\phi_f(P), [x_b]\phi_a(P)\big) \mid P \in E_0[B]\}$$

is maximal isotropic for the B-Weil pairing.

Proof. We do the verification, for all $P, Q \in E_0[B]$:

$$\begin{aligned} e_{E_f}\big(\phi_f(P), \phi_f(Q)\big) e_{E_a}\big([x_b]\phi_a(P), [x_b]\phi_a(Q)\big) &= e_{E_0}(P,Q)^f e_0(x_b.P, x_b.Q)^A \\ &= e_{E_0}(P,Q)^f e_0(P,Q)^{x_b^2 A} \\ &= e_{E_0}(P,Q)^{f + x_b^2 A} \\ &= e_{E_0}(P,Q)^{f+A} \quad \text{because } \; x_b^2 \equiv 1\,[B] \\ &= 1 \quad \text{because } \; f + A = B. \end{aligned}$$

And since ϕ_f and $[x_b]\phi_a$ have degree prime to B, they are injective on $E_0[B]$, consequently $\#G = \#E_0[B] = B^2$. □

Let us look at the changes that this additional assumption brings. In the first part of the algorithm we test whether K is diagonal. If it is, we compute (f_{ij}) directly thanks to Proposition 2.2.1. Now, we can assume that K is not diagonal. Thus by Proposition 2.2.2, we have a solution (f_{ij}) where every isogeny is non-zero. So their degrees are well defined, and we do an exhaustive search on the degrees of the f_{ij}.

With Proposition 2.2.3, we can reduce the number of loops on *degs*, the quadruplets of integers representing the possible degrees of the 1-dimensional isogenies in the matrix. This significantly improves the efficiency of our algorithm, since a lot of computations are done for each 4-tuples of degrees. It can be compared to the **Step 2** of the previous section.

```
for degs in { ls : ld in CartesianPower({1..S}, 4)
              | Max(ls) eq S
                 /* Avoid permutations of rows: */
              and ((ls[1] lt ls[3]) or (ls[1] eq ls[3] and ls[2] le ls[4]))
                 /* results on maximal isotropic kernel: */
              and (ls[1]+ls[2]) mod l eq 0
              and (ls[3]+ls[4]) mod l eq 0
              where ls is [ld[i] : i in [1..4]] } do

        /* Here we know that the matrix does not have any 0 in it */


        candidates_jFullMatrix := {[a, b] : a in candidates_j_1[degs[1]],
```

```
                                                    b in candidates_j_1[degs[3]]
                                    | a in candidates_j_2[degs[2]] and
                                      b in candidates_j_2[degs[4]] };


        if IsEmpty(candidates_jFullMatrix)
                then continue;
        end if;
```

Moreover with Proposition 2.2.2, we do not have to check all the possible triangular matrices, and we know that $\langle P, Q\rangle$ is diagonal if and only if the returned matrix is diagonal. Since we have checked this before, we only have to look for full matrices. This observation saves us a lot of calculation time.

2.2.3 Issues faced

During this internship, we encountered some difficulties. We give here the most important ones, starting with practical problems.

In theory we often work *up to isomorphism*, which is no longer possible in the implementation, since we want to evaluate the isogenies we have constructed. For example, suppose we construct f_{11} and f_{12} with Vélu's formula, and we want to try it as the first row of a solution. We want to test this: $\forall (P_1, P_2) \in K,\ f_{11}(P_1) + f_{12}(P_2) = 0$. But it may happen that the codomains of f_{11} and f_{21} are not equal, even if they are isomorphic. So to do the addition " + ", we have to compute isomorphisms $\phi_i : \text{Codomain}(f_{ij}) \to E_i'$. But composing isogenies can be very expensive, so we represent the result of **NaiveResearch** as $\big([f_{ij}], \phi_1, \phi_2\big)$. Instead of just $[g_{ij}]$, with $g_{i1} = \phi_i \circ f_{i1}$.

Also, to be precise, our algorithm returns a (matrix representation of an) isogeny F which vanishes on the kernel input, but we have to check if it vanishes *exactly* on it. This is not a trivial problem, because the exhaustive way of checking that F is not 0 at all other points of the product of elliptic curves is not effective. Indeed there is too much points to consider. To avoid this issue, we have tried to use the rational functions defining the returned isogenies $[f_{ij}]$, to build a test using Gröbner basis. Unfortunately we are having trouble implementing the test. MAGMA gives us access to the rational functions that define an isogeny through primitives. But in our case we are using these primitives in a way that the designers probably did not anticipate. We are therefore confronted with bugs that we cannot work around at the moment. Moreover even if the matrix (f_{ij}) vanishes exactly on K it may not be an isogeny, here is an example. If we found $f_{11} : E_1 \to E_1'$ and $f_{12} : E_2 \to E_1'$ such that for every $(P, Q) \in K$ we have:

$$f_{11}(P) + f_{12}(Q) = 0.$$

Then the matrix $\begin{pmatrix} f_{11} & f_{12} \\ g \circ f_{11} & g \circ f_{12} \end{pmatrix}$, for any morphism $g : E_1 \to E'$, is a *morphism* (but not an isogeny, because of the lack of surjectivity) which vanishes on K. We have to exclude those cases.

Another major problem is that our general algorithm is still slow. There are two main reasons for this; firstly, there is the double loop on the degrees and the j-invariants, which involves a very large number of iterations. And second, the later tests can involve expensive computations, for example when we construct candidates for the $[f_{ij}]$ which are not cyclic.

Finally, a major theoretical problem remains: we have no bounds on the degree of $f_{11}, \dots, f_{22}$. This would help us prove an upper bound on the complexity of our algorithm. We hope that such a bound could be polynomial in the cardinality of the finite subgroup K. Let us describe what we are looking for. Given an integer B, we hope to find a polynomial $P \in \mathbb{Z}[X]$ such that, for every finite group K of cardinality B^2, there exists a matrix representation (f_{ij}) of an isogeny whose kernel is exactly K that satisfies:

$$\max_{i,j\in\{1,2\}} \deg(f_{ij}) \leq P(B) \tag{2.2}$$

2.2.4 Perspectives

Before concluding with some open questions about this work, let us summarize its content. After giving a non-exhaustive overview of the cryptography around SIDH in Chapter 1, we turned our attention to the construction of isogenies between maximal product surfaces. In Section 2.1.2 we presented a first algorithm that was far from satisfactory. However, thanks to the theory of polarized abelian varieties (Section 1.2), we proved some properties in Section 2.2.1 which helped us to implement a better algorithm. Let us describe it one last time. We fix maximal supersingular elliptic curves E_1, E_2 over a finite field $\mathbb{F}_{p^2}$. Let K denote a rational finite subgroup $K \subset (E_1 \times E_2)[\ell]$ of order ℓ^2, with ℓ a prime distinct from p. We assume that K is maximal isotropic for the $(\ell, \lambda_1 \otimes \lambda_2)$-Weil pairing, where λ_i is the canonical principal polarization on E_i. We use a brute-force like algorithm to find four morphisms $(f_{ij})_{i,j\in\{1,2\}}$ and two isomorphisms $(\phi_i)_{i\in\{1,2\}}$ such that the matrix $\begin{pmatrix} \phi_1 \circ f_{11} & f_{12} \\ \phi_2 \circ f_{21} & f_{22} \end{pmatrix}$ represents an isogeny between product surfaces, that vanish on K.

One of the main questions that arises is the following. In the vast majority of examples, if we denote by (d_{ij}) the degree of (f_{ij}), then $[d_{11}, \dots, d_{22}]$ is of the form:

$$[u, v, u, v] \quad \text{or} \quad [u, v, v, u]$$

with $u, v \in \mathbb{N}$. A crucial question is to understand why such lists arise and what we can say about the coefficients u, v. Can they be bounded by a polynomial in B as in Equation 2.2? Is there another relation between the d_{ij} than the one given by Proposition 2.2.3? Why are there other types of quadruplets?

Second, we saw that it is easier to compute matrix of isogenies from a maximal isotropic kernel for the Weil pairing with respect to the product polarization. What happens for other polarizations ? It seems to be a deep question. For example, in the context of Part 2.1.2 and with the notation of the second paragraph, there exists a maximal isotropic kernel K with $\mathrm{Card}(K) = B^2 = (\ell_1\ell_2)^2$. This kernel leads to another maximal isotropic kernel $K_{\ell_1} = B/\ell_1 \cdot K$ which defined a 2-dimensional isogeny F_1. But $F_1(K)$ may not be maximal isotropic for the product polarization. Thus we cannot iterate the protocol in this special case. But is there a polarization on the codomain of F_1 that gives F_1 and $F_1(K)$ good properties? Is it computable?

Finally, in [LR] we find other ways to construct isogenies between abelian varieties, knowing their kernel. The authors use a rather deep theory to answer this question in a very general framework. One of the next steps in our work will be to understand their paper and see how well it fits our constraints.

Bibliography

[BCP] Wieb Bosma, John Cannon, Catherine Playoust. The magma algebra system I: The User Language. *Journal of Symbolic Computation*, 24(3):235–265, 1997.

[CD] Wouter Castryck, Thomas Decru. An efficient key recovery attack on SIDH. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 423–447. Springer, 2023.

[CFA] Henri Cohen, Gerhard Frey, Roberto M. Avanzi. *Handbook of elliptic and hyperelliptic curve cryptography*. Taylor and Francis, 2006.

[DH] Whitfield Diffie, Martin E. Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

[Feo] Luca De Feo. Mathematics of isogeny based cryptography, 2017. Lecture notes available at https://defeo.lu/research.

[FJP] Luca De Feo, David Jao, Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3):209–247, 2014.

[FMP] Tako Boris Fouotsa, Tomoki Moriya, Christophe Petit. M-SIDH and MD-SIDH: countering SIDH attacks by masking information. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 282–309. Springer, 2023.

[GB] Damien Robert Gaetan Bisson, Romain Cosset. Avisogenies a library for computing isogenies between abelian varieties. https://www.math.u-bordeaux.fr/ damienrobert/avisogenies/, Latest version released on 2021-03-13.

[HS] Marc Hindry, Joseph H. Silverman. *Diophantine Geometry: An Introduction*. Springer New York, NY, 2000.

[JKP$^+$] Bruce W. Jordan, Allan G. Keeton, Bjorn Poonen, Eric M. Rains, Nicholas Shepherd-Barron, John T. Tate. Abelian varieties isogenous to a power of an elliptic curve. *Compositio Mathematica*, 154(5):934–959, 2018.

[Kan1] Ernst Kani. The number of curves of genus two with elliptic differentials. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 1997:122 – 93, 1997.

[Kan2] Ernst Kani. Products of CM elliptic curves. *Collectanea mathematica*, 62(3):297–339, 2011.

[Kan3] Ernst Kani. The moduli spaces of Jacobians isomorphic to a product of two elliptic curves. *Journal of Number Theory*, 139:138–174, 06 2014.

[LPS] Alexander Lubotzky, Ralph Phillips, Peter Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.

[LR] David Lubicz, Damien Robert. Computing isogenies between abelian varieties. *Compositio Mathematica*, 148(5):1483–1515, 2012.

[Mil] James S. Milne. Abelian varieties (v2.00), 2008. Lecture notes available at www.jmilne.org/math/.

[MMP+] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, Benjamin Wesolowski. A direct key recovery attack on SIDH. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 448–471. Springer, 2023.

[Mum] David Mumford. *Abelian Varieties. Tata Institute of Fundamental Research Studies in Mathematics, no. 5.* Oxford University Press, 1970.

[Rob] Damien Robert. Breaking SIDH in polynomial time. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 472–503. Springer, 2023.

[Sam] Pierre Samuel. *Théorie algébrique des nombres.* Hermann, 1967.

[Sho] Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134, 1994.

[Sil] Joseph H. Silverman. *The Arithmetic of Elliptic Curves.* Springer, 2009.

[Was] Lawrence C. Washington. *Elliptic curves: number theory and cryptography.* CRC press, 2008.